The new general data protection regulation

de Hert, Paul; Papakonstantinou, Vagelis

Published in:
Computer Law and Security Review

Publication date:
2016

Document Version
Peer reviewed version

COMPUTER LAW & SECURITY REVIEW 32 (2016) 179–194

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The new General Data Protection Regulation: Still a sound system for the protection of individuals?

Paul de Hert [a,b,*], *Vagelis Papakonstantinou* [a,*]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *Tilburg University (Tilt), The Netherlands*

Keywords:
EU General Data Protection Regulation
Controller–processor relationship
Internet of things
Individual consent
DPIAs
The right to be forgotten
Data portability
Personal data breach notifications

A B S T R A C T

The five-year wait is finally over; a few days before expiration of 2015 the "trilogue" that had started a few months earlier between the Commission, the Council and the Parliament suddenly bore fruit and the EU data protection reform package has finally been concluded. As planned since the beginning of this effort a Regulation, the General Data Protection Regulation is going to replace the 1995 Directive and a Directive, the Police and Criminal Justice Data Protection Directive, the 2008 Data Protection Framework Decision. In this way a long process that started as early as in 2009, peaked in early 2012, and required another three years to pass through the Parliament's and the Council's scrutiny is finished. Whether this reform package and its end-result is cause to celebrate or to lament depends on the perspective, the interests and the expectations of the beholder. Four years ago we published an article in this journal under the title "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals". This paper essentially constitutes a continuation of that article: now that the General Data Protection Regulation's final provisions are at hand it is possible to present differences with the first draft prepared by the Commission, to discuss the issues raised through its law-making passage over the past few years, and to attempt to assess the effectiveness of its final provisions in relation to their declared purposes.

1. Introduction: a thorough reform but based on ideas already bypassed?

The five-year wait is finally over; a few days before expiration of 2015 the "trilogue" that had started a few months earlier between the Commission, the Council and the Parliament suddenly bore fruit and the EU data protection reform package has finally been concluded. As planned since the beginning of this effort a Regulation, the General Data Protection Regulation (henceforth, the Regulation[1]) is going to replace the 1995 Directive[2] and a Directive, the Police and Criminal Justice Data

* *Corresponding authors*. Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussels, Belgium.
E-mail addresses: paul.de.hert@vub.ac.be, paul.de.hert@uvt.nl (P. de Hert); vpapakonstantinou@mplegal.gr (V. Papakonstantinou).
http://dx.doi.org/10.1016/j.clsr.2016.02.006

[1] The text referred to in this article is the compromise text reached after conclusion of the inter-institutional negotiations (*trilogue*) between the Commission, the Council and the Parliament, as made available online by the Parliament's LIBE Committee on 17 December 2015. Readers are advised that this text will be different from the final text both in terms of numbering (a number of articles and preamble paragraphs in the compromise text are deleted or numbered inconsequentially) and in terms of wording (linguistic processing pending).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, pp. 31–50.

Protection Directive (henceforth, the Directive[3]), the 2008 Data Protection Framework Decision.[4] In this way a long process that started as early as in 2009, through a relevant public consultation launched by the Commission, peaked in early 2012, when the Commission published its own proposals, and required another three years to pass through the Parliament's and the Council's scrutiny is finished. Whether this reform package and its end-result is cause to celebrate or to lament depends on the perspective, the interests and the expectations of the beholder. This paper will attempt a first assessment of one of its components, the Regulation, in this regard.

There is very little personal data processing that will remain unaffected by the combined effect of the Regulation and the Directive. Their combined scope covers all personal data processing executed by private actors as well as all similar processing undertaken by law enforcement agencies in the Member States; in fact, only processing by secret agencies for national security purposes[5] and processing by EU law enforcement agencies is left unregulated. Apart from these exceptions, there will practically be no individual within the EU not directly affected by the reform. The new instruments are therefore expected to affect the way Europeans work and live together. However, these two instruments are only part of the EU data protection reform effort: at the same time important legislative initiatives have been undertaken with regard to Eurojust,[6] Europol[7] and the soon-to-be-founded European Public Prosecutor Office.[8] Sector-specific legislation also currently under elaboration refers to the EU PNR Directive,[9] while it should also be noted that Regulation 45/2001, establishing the European Data Protection Supervisor, also eagerly awaits its (promised) revision.[10] Once all of the above have been enacted nothing in the EU data protection edifice will remain the same.[11]

A critical observer might note that the ideas behind the Regulation and the Directive go back to 2012 and that already all circumstances within which they were drafted have in the meantime changed substantially. From a political point of view, public debt, the war against terrorism and immigration have dominated the EU agenda over the past few years; data protection is found right in the centre of relevant debates, when for instance processing personal data of immigrants or alleged terrorists or when overstretching the limits of already exhausted Data Protection Authorities to cover each and every new type of personal data processing within their respective jurisdictions. Recent terrorist attacks in EU capitals have also affected social perceptions, with the emphasis being once again, as was the case back in 2001, on security rather than human rights.[12] Even technology has changed substantially within the past five years: smartphones and apps have carved up an important part in users' preferences over the open internet; the open internet itself is distinguished from the "dark" internet where supposedly all types of criminal activity takes place; cyber security incidents have occurred at an unprecedented pace at all levels, meaning both at corporate and at state level; big data, drones, the internet of things and other niche technologies constantly challenge the limits of legislation.

On the other hand EU case law has not stayed idle, calmly waiting for the new provisions of the EU data protection reform package to be finalised and come into effect. On the contrary, the Court of Justice of the European Union (CJEU) has over the recent past undertaken a substantial effort to protect individual data protection even, when needed, stretching the already exhausted provisions of the 1995 Directive to their real and imaginative limits.[13] In this way, however, notions such as the right to be forgotten or extraterritoriality or international data transfers that are treated in the text of the new legislative instruments should not be considered as newcomers in the EU. In fact quite the opposite is true, because useful experience

[3] Compromise text also made available by the LIBE Committee on 17 December 2015, as above.

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60, 30.12.2008.

[5] See Art. 2 of the Regulation and of the Directive respectively.

[6] Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM/2013/0535 final.

[7] Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final. At the time of drafting this article the trilogue stage was also completed on this Regulation; therefore, its formal adoption is also pending.

[8] Proposal for a Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final.

[9] Provisional text drafted by the Commission (based on its (rejected) initial draft: Proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final) also approved by the Parliament and the Council on 2 December 2015.

[10] A promise also undertaken in the text of the Regulation itself; see Preamble 14a.

[11] The regional and global scene ought also not be overlooked: The Council of Europe 1981 Convention, to which all EU Member States are signatory parties, is also currently in the process of being amended (see relevant Council of Europe webpages (Modernisation of Convention no.108, at www.coe.int); the OECD Guidelines have been revised only in 2013 (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

[12] See The Economist, The terrorist in the data – how to balance security with privacy after the Paris attacks, 28 November 2015.

[13] Reference is made here to the important cases of Schrems (Maximillian Schrems v Data Protection Commissioner, C-362/14), Weltimmo (Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14), Google Spain (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12), and data retention directive (Digital Rights Ireland and Seitlinger and Others, Judgment in Joined Cases C-293/12 and C-594/12). Perhaps this important pro-data protection trend can be explained by the fact that the Regulation is substituting a Directive and hence at least from a German point of view judicial redress for individuals becomes automatically limited (see Hornung G, A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft on 25 January 2012, SCRIPTed Vol. 9 issue 1, 2012, p. 67).

has been accumulated through application of recent groundbreaking case law on data protection that could put the Regulation's and the Directive's provisions, once in effect, in good standing.

All of the above could not possibly shadow the fact that a herculean law-making effort has been successfully concluded. The Regulation is a text of some 90 articles attempting to regulate through its direct effect, itself an unprecedented attempt in such a field, any personal data processing undertaken by controllers other than these of the Directive. Printed out, it occupies around 200 pages. While working on it, the Parliament attracted around 4000 amendment proposals.[14] EU lobbying allegedly reached unprecedented levels.[15] Neither is the law-making effort concluded yet: tens of delegated acts need to be issued by the Commission; Member States need to amend their national legislation in order to accommodate the Regulation's needs. The two-year period for the Regulation to come into effect will definitely constitute a busy and equally interesting law-making period; in this case, in view of its direct effect, details matter.

Four years ago we published an article in this journal under the title "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals".[16] In it we focused on eleven aspects of the then draft Regulation, in its initial version as released by the Commission, and made a relevant short presentation attempting to present the *raison d' être* of the Commission's proposals and assess their usefulness for the future from a data protection point of view. The reasoning behind the choice of these aspects as well as the reasons for the data protection reform effectuated through introduction of the Regulation and the Directive can be found therein. This paper essentially constitutes a continuation of that article: now that the Regulation's final provisions are at hand it is possible to present differences since the first draft prepared by the Commission, to discuss the issues raised through its law-making passage over the past few years, and to attempt to assess the effectiveness of its final provisions in relation to their declared purposes. While doing this attention will primarily be given to the three drafts that entered the *trilogue* stage, meaning these produced by the Commission, the Parliament and the Council respectively. Our point of view will once again be guided towards better serving the data protection purposes. In this way we hope that the groundwork will start being laid for what is expected to be a long and fruitful legislators', academics' and practitioners' exchange on the numerous issues raised by the Regulation.

2. The law-making process: a brief history

Because this paper is intended to recap a law-making process that lasted more than five years, we consider it important to remind and note down its basic steps: work on the amendment of the 1995 Directive began as early as 2009, through release of a relevant public consultation by the Commission. Among the reasons listed for the need to amend it the most important ones were probably its technologically out of date status as well as the lack of harmonisation among Member States. At any event, the Commission released a relevant Communication in 2010.[17] Subsequently all major participants in the process (the Council, the Parliament, the EDPS and the Article 29 Working Party) published their views.[18] Finally, this first stage was concluded in early 2012,[19] when the Commission released its drafts for the Regulation and the Directive respectively.[20]

Work was subsequently passed on to the Council and the Parliament, who took turns in amending the Commission's above two drafts. In the Parliament this task was assigned to its Committee on Civil Liberties, Justice and Home Affairs ("LIBE") that in turn assigned one rapporteur for each text.[21] Allegedly due to pressure from unrelated factors (the June 2014 elections were listed among them) the Parliament hurried to release its own views on each text in early 2013.[22]

On the other hand, the Council took substantially longer to react: having assigned work to its EU Council's Working Party on Information Exchange and Data Protection, known as the "DAPIX" committee, it expanded its work over three years, six presidencies (Cyprus, Ireland, Lithuania, Greece, Italy, Latvia) and innumerable meetings (most of them admittedly devoted to the Regulation rather than the Directive). It finally reached its final position on 15 June 2015[23]; however it should be taken into account that the Council, because of its prolonged processing of the two documents, did not regulate only on the basis of the initial Commission draft, but it also had at hand the Parliament's finalised opinion as well. In practice this meant that, keeping the *trilogue* stage in mind, it would not be feasible for it to deviate substantially from the other two already formulated and submitted opinions that would officially have later to reach compromise with its own. In addition, again because of the prolonged period for processing, it is the Council that was the indirect recipient of the important CJEU case law mentioned above that kept pointing emphatically towards a pro-data protection perspective.

The *trilogue* that followed perhaps took less time than expected: the Commission announced the final conclusion of the process on 16 December 2015. Factors that may, or may equally have not, effected such speed may include the CJEU Schrems

[14] See Data Protection Regulation provokes intense lobbying, EJC News, v49 issue 7/8, July/August 2013.

[15] Ibid.

[16] Computer Law & Security Review 28 (2012).

[17] A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final.

[18] See footnotes no.11–14 in our previous paper.

[19] Important information particularly with regard to the policy option then at hand may also be found in the Commission's Impact Assessment report (SEC(2012) 72 final, 25.01.2012).

[20] A leaked version was made available on November 2011 that differed substantially to the final one (see Hornung G, ibid, p. 66).

[21] Jan-Philipp Albrecht, rapporteur for the Regulation and Dimitrios Droutsas, rapporteur for the proposed Data Protection Directive for the law enforcement sector.

[22] LIBE reports A7-0402/2013 and A7-0403/2013 (22.11.2013) for the Regulation and the Directive respectively. See also Burton C/Kuner C/Pateraki A, The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report, Privacy & Security Law Report, 12 PVLR 99, 01/21/2013.

[23] Council of the European Union, 9565/15.

case law that annulled the Safe Harbour Agreement with the USA, the Paris terrorist attacks, or the quick pace that the EU PNR Directive gained in their aftermath.[24] At any event, while the final *trilogue* compromise text is already known, and is used as the basis for this article, it is expected that the Regulation and the Directive will have been formally approved and will have finished with their language processing and gained their final numbers by mid-2016.

3. The choice of legal instruments: an unprecedented choice (and an important win for the Commission)

The importance of the choice for the legal instruments to bear the burden of regulating EU data protection cannot be emphasised enough: to our mind, perhaps the most important contribution to EU personal data processing by the Regulation is the choice of instrument itself, regardless of its final provisions (a statement that is of course not altogether true because, as it will be later demonstrated, its provisions present data protection merit also in themselves). A Regulation to replace the 1995 Directive means, *prima facie*, that harmonisation problems of the past will no longer occur. Although a complex consistency mechanism is established in order to gloss out differences among Member States, the effectiveness of which one can only wait to witness in practice, the fact is that a Regulation's primary concern, and consequently a guiding principle during its application, refers to achieving a harmonised data protection approach among Member States. Given the globalisation of personal data processing and the recent forum shopping, in one way or another, practiced by internet (USA) companies, this seems a reasonable, if not necessary policy option.

On the other hand, the significance of this unprecedented policy option for EU law to enter Member State level through a Regulation on such a broad field as data protection ought not to be overlooked.[25] Regulations are direct effect legal instruments. Until today they have been used in niche or in any way restricted fields such as, for instance, competition law, the establishment and management of EU agencies, or the regulation of the EU trademark. In all other fields a Directive, as was the case with the 1995 Directive, was deemed a preferable solution, leaving space for implementation to Member States. However, this is no longer the case in the data protection field. A Regulation, expressly intended to find direct application in Member States, is opted for in order to regulate the vast majority of personal data processing. A Directive is from now on suitable only for processing undertaken by law enforcement agencies. This inevitably signals an important qualitative change: data protection is no longer perceived as a local phenomenon, to be regulated according to local legislation with an EU Directive only issuing high-level instructions and guidelines. On the opposite, data protection is considered from now on an EU concern, to be regulated directly at EU level in a common manner for all Member States through a Regulation. The regulation of EU data protection through a Regulation rather than a Directive constitutes a turning point for EU data protection (potentially also for all of EU law, depending on its ultimate success) signalling, to our mind, a forced exit of this particular field of law from Member State level to EU level.[26]

This choice of legal instruments should be accredited to the Commission. Not only did it introduce them in its initial proposal back in 2012, but it also insisted in its opinion even when, as was frequently the case during the law-making process, many Member States doubted this policy option. However, the Commission insisted, and its point of view finally prevailed: the final outcome of the long law-making negotiations found the Regulation (and the Directive, respectively) preserved despite frequent hostility against it.

Admittedly, the choice of legal instruments is not only cause for celebration, at least not until we have witnessed their success in practice. The Regulation will come into effect within two years after its publication.[27] This intermediate period is not a time to patiently wait. Instead, it is expected to be a particularly busy time for all EU institutions, because they will have to prepare all the implementing acts needed. The Regulation has set itself an ambitious task: the coordination of twenty-eight Member States, their respective Data Protection Authorities, national laws and courts is by no means an easy task. Its consistency mechanism may or may not work. The bar of expectations has been raised high: the Commission has promised nothing less than a "strong, clear and uniform legislative framework at EU level" that, among others, will "do away with the patchwork of legal regimes across the 27 member states and remove barriers to market entry".[28] But what does that mean exactly? Does it mean that multinational companies will be faced with exactly the same approach (rules and regulations are only one part of it) across the EU? Does it mean that a given type of processing will be treated in exactly the same way in all jurisdictions across the EU? Could it also mean that the same penalties will be imposed upon data controllers and the same remedies will be paid to data subjects in the event of same-type data protection infringements across the EU? Could it also involve same-speed processing of requests in various Data Protection Authorities across the EU? Or, same costs for implementation for data controllers no matter where they reside in the EU? Only the listing of the above potential expectations hosted under the "harmonised implementation" promise undertaken by the Regulation serves to remind us the complexity of the task at hand – and its very real possibility to fail.

[24] See de Hert P/Papakonstantinou V, Repeating the Mistakes of the Past Will do Little Good for Air Passengers in the EU. The Comeback of the EU PNR Directive and a Lawyer's duty to Regulate Profiling, New Journal of European Criminal Law, Vol. 6, Issue 2, 2015.

[25] See Blume P/Svanberg C W, The Proposed Data Protection Regulation, Cambridge Yearbook of European Legal Studies, 1/15, 2013, p. 34.

[26] A fact that did not go unnoticed, see J Masing, Ein Abschied von den Grundrechten, Süddeutsche Zeitung (2012), 9 January 2012, and Hornung G, ibid, p. 67.

[27] See Article 91.

[28] See Reding V, The European Data Protection Framework for the Twenty-First Century, International Data Privacy Law 2012, Vol. 2, No. 3, p. 128.

4. Personal data and sensitive personal data (Art. 4 and 9 of the Regulation)

The question, what exactly constitutes "personal data", is crucial for the data protection purposes, because only what qualifies under basic data protection law as such is regulated by it. All other data, regardless whether perceived as personal or not, falls outside its scope. In the 1995 Directive use was made of a phrase that proved resilient over the past twenty years: "personal data shall mean any information relating to an identified or identifiable natural person ('data subject')" (Art.2). In principle this distinction was upheld in the Regulation as well. However, while what is an identified individual is more or less clear, over the past years extensive debates were devoted on what exactly such "identifiability" included or not. The Article 29 Working Party had in particular developed a rather expansive approach on this matter[29] and the text of the Regulation more or less seems to adopt the same approach, in its Article 4(1). This wording does not differ substantially from the initial provided by the Commission; apparently, a need was identified by all three law-making bodies to detail what an "identifiable" person is, but the initial approach of the Commission appeared sufficient to this end. Further guidance is provided in the Recitals: in particular, a proportionality test is introduced (identifiability is relative to "the means reasonably likely to be used" taking account of "all objective factors" such as technology, effort and cost) in order to assess each time what data may pertain to identifiable individuals: if the test is not passed, then such data are considered anonymous and the law does not apply on them.[30]

While work on "personal data" more or less updated what was already perceived in the 1995 Directive and did not derogate much from the Commission's initial proposal, the newcomer in the field is "pseudonymisation" and "pseudonymous data". Indeed, no mention of such process or type of data may be found anywhere in the Commission's initial drafts. It is therefore an addition made first by the Parliament[31] that was also upheld by the Council. In essence, "pseudonymisation means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person" (Art. 4(3b)). The relationship between pseudonymous data and personal data, meaning whether the former is a subcategory of the latter and therefore falls under the Regulation's scope or not, is given in the Recitals: "Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person" (23). However, because they are considered information on an identifiable person, the proportionality test above, applied particularly on the "separate additional information" ought to be applied – presumably there can be a case where pseudonymous data should not be considered as personal data for the purposes of the data protection legislation. Other additions in the final text of the Regulation, apparently accountable to Council input, refer to the information on deceased persons.[32]

With regard to sensitive data, here again the 1995 Directive's approach is basically maintained in the text of the Regulation as well. Namely, the past schematic distinction between common and sensitive ("special categories of") personal data is upheld in the Regulation too: according to it, personal data are distinguished according to their nature, meaning what they "reveal": these "revealing" information on any one of the categories listed in the respective provisions are separated from the rest (not "revealing" any of the above) and are treated differently. The problem here is that, depending on the processing circumstances, common data may be used to reveal sensitive information, for instance surnames or meal preferences revealing religion or race. While the verb "revealing", as after all included already since 1995 in the text of the Directive, could denote a dynamic interpretation that could be adapted to processing circumstances, this has not proved to be the case in the past: instead, personal data were distinguished into common or sensitive on the basis of its nature and not its potential uses. This problem will presumably continue to occur under the Regulation as well.

Apart from this issue, the Regulation includes, as is by now customary in data protection instruments, a general prohibition for the processing of sensitive data, in par. 1 of Article 9, accompanied by exemptions, in par. 2 of the same Article. Sensitive data are these revealing "*racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation*". In relation to the 1995 Directive's listing the only change can be traced in the addition of genetic data, biometric data and sexual orientation data. Only the first two categories are defined in Article 4 of the Regulation; they constitute additions in the data protection field that come as a result of scientific developments in their respective fields. All remaining categories apparently had a smooth pass from the 1995 to the Regulation: the Parliament and the Council made very few changes to the Commission's initial proposal. Exemptions, meaning cases when personal data processing is allowed despite of the fact that sensitive data are being processed, refer to a number of cases, among which are consent, the protection of vital interests of the individual, preventive or occupational medicine, or public interest. Here again the list is similar to that of the 1995 Directive and here too the Commission's initial proposal was more or less upheld by the other two bodies.

The main difference brought to the Commission's initial proposal refers to the separation from the above categories of sensitive data of "data relating to criminal convictions and offences or related security measures based on Article 6(1)". While in the initial Commission proposal these data were listed among the above general sensitive data categories, after intervention by the other law-making bodies (apparently it was the Council's approach that prevailed) they were singled out and

[29] See Opinion 4/2007.

[30] See Recital 23.

[31] That also added "encrypted data" that however did not make it into the Regulation's final version.

[32] Upon which the Regulation does not apply, see Recital 23aa.

received separate treatment, in Article 9a, their processing is only allowed under the control of an official authority or after adequate safeguards have been provided for by Member State law. This appears to be a justified approach: the space for exemptions provided under Article 9 is wide and criminal records may constitute in practice popular requests (for instance, by employers), leading to doubts on whether one or more of these exemptions applies to such data (for example, would individual consent suffice to reveal criminal records? How about the exercise of legal claims?). However, if customised protection is granted to a single category of sensitive data, that of criminal records, the obvious question that follows is why not each one of them received similar, specialised treatment; after all, similar concerns in relation to the list of exemptions in par. 2 of Article 9 could be raised about all of them.[33]

5. The personal data processing actors (Art. 4 of the Regulation): an anachronism in the text of the Regulation

Neither did the Regulation deviate substantially from the 1995 Directive in the case of the personal data processing actors: the well-known system of data subjects, controllers, processors, recipients and third parties is more or less maintained in its text (in Article 4). It should also be noted that the initial Commission's proposal went more or less undisputed on this matter by the other two law-making bodies. In this way, however, the 1995 Directive's terminology and, what is more important, understanding of personal data processing remain intact. Apparently, to the Regulation's drafter's mind nothing has changed in the basic personal data processing scheme over the past forty years (keeping in mind that the 1995 Directive adopted the scheme that was found in the first data protection acts released during the 1970s).

The Regulation in this way appears to be consistent with, or stuck to, its 1970s roots. Back then a new piece of legislation that regulated a new technology was probably felt that it had to apply new terminology as well. This corresponded to the then conceivable personal data processing scheme: on the one side of the spectrum individuals were named data subjects most likely because a certain level of abstraction was needed to separate an individual from its personal data. No matter how awkward, and probably unnecessary by now, their naming has stuck: individuals (natural persons) who are the recipients of the right to data protection will apparently continue to be called data subjects in the long run – an approach unjustified also in terms of Article 16 TFEU that does not refer to "data subjects" but to "individuals" instead.

On the other side of the spectrum we have those who run the processing operations: controllers, processors, recipients and third parties. Back in the 1970s it was conceivable that while some entity made the choices for the processing another entity may be chosen by it to carry it out. Mere recipients of the information and third parties somehow connected to the whole process could also be involved. The Regulation maintained this scheme and its corresponding terminology. While this might appear a consequent policy option, in line with what has been known in the data protection field for the past decades, it is likely not to be compatible with the contemporary processing reality. In specific, the basic distinction between controllers, who decide on the "purpose and means" of the processing and all their other types of helpers (processors, recipients and third parties), is most likely no longer sustainable in current processing circumstances: not only is the identification of a single entity as the source of a processing operation impossible in many cases, as it will be demonstrated immediately below, but even if that was the case it is not clear that all intermediate participants in the same processing should remain unaccountable for it. In other words, the basic assumption[34] that a controller is always identifiable and accountable and it is up to him to decide whether to assign processing to a data processor or other parties, who therefore remain passive in the process, is no longer the case in contemporary processing environments. Under cloud computing or big data processing, for instance, processors are at least of equal importance (if not more significant, if they happen to be multinational service providers) as controllers.

The real problem however is that this concept of personal data processing is hopelessly static: it places at its basis an identifiable, single, standalone personal data processing operation. We believe that this is an outdated approach: while back in the 1970s, when this model was devised, indeed this was the case (it was also held back then that a dozen of computers would suffice for all humanity) and perhaps under the advent of the internet the only thing that changed was the volume of these otherwise standalone operations; this is no longer the case in the era of big data and the internet of things. Ubiquitous computing means ubiquitous personal data processing. Machines, everything from smartphones, computers and televisions to vacuum cleaners, fridges and coffee makers, are programmed by design to process information constantly just for the sake of it – meaning, for no apparent from the beginning purpose as required by the purpose specification principle.[35] The idea that each one of these processing operations could be singled out identified and attributed to a particular entity, in order for accountability to be established, is simply unattainable. For example, in the case of the internet of things, who would such a data controller be? The company that manufactured the coffee maker? The household that has installed it and operates it? The utility service that monitors its operation in order to shut it down if idle for too long? Or the service provider that also monitors its processing in order, for instance, to better service it or feed it with more coffee? The idea of a single data controller that will carry all liability under data protection law while all other parties to the same processing carry less or no responsibility at all is outdated and lacks an understanding of where technology and lifestyles are headed.

[33] For instance, with regard to biometric data special attention needs to be given to the fact that only these "uniquely identifying a person" are considered sensitive data, leaving therefore the important category of behavioural biometric data outside the scope of protection (see Gayrel C, Modernisation of Convention 108, ERA Data Protection Conference, 11 May 2015).

[34] See also the Article 29 Data Protection Working Party Opinion 1/2010.

[35] Thankfully, the purpose specification principle has taken that into account; see the analysis that immediately follows.

Admittedly, the Regulation did make a significant contribution in personal data processing role allocation, by introducing "joint controllers" in the scene. These are to be found "where two or more controllers jointly determine the purposes and means of the processing of personal data".[36] While this is a sound idea that indeed corresponds to contemporary processing complexity, the fact remains that the multitude of auxiliary players on the same side of the processing (processors, recipients, third parties) adds little to clarity and brings limited added value to the data protection purposes.

This is why we believe that the preferable way forward would have been a bold deletion of all secondary roles in the personal data processing process except that of the data controller: the roles of processors, recipients and third parties are difficult to award and may ultimately only be perceived as favourable treatment to certain industries – including in the case of the Regulation the public sector that is taken care in its text to constitute a mere recipient if acting within its normal course of activities (see also Recital 24). By having too many roles inserted on the data processing end, the Regulation has trapped Data Protection Authorities into endless investigations on the actual roles of the parties involved in any given processing, while expectedly contractual clauses and other legal tricks will be brought in to blur the boundaries between them. To our mind there is no particular reason why participants in one way or another in a personal data processing operation should carry less or no responsibility to observe the Regulation's provisions. Regardless whether acting on command by a third party or on its own initiative, and regardless whether it is an infrastructures service provider or a single party executing a specific type of processing, obligations towards the law ought to be the same. This after all would have been what is expected from the side of data subjects that cannot and should not be forced to enter each time into the contractual and operational relationships among data controllers in order to establish accountability for processing their personal data. The roles of processor, recipients and third party offer nothing more to the data protection environment than convenient escape vehicles for industries seeking a free ride to personal data processing without carrying any data protection obligations. The Regulation seems to reward their aspirations.

6. Reforming the Directive's principles: important additions to an essentially preserved processing system (Articles 5 and 6 of the Regulation)

The fundamental importance of Articles 6 and 7 of the 1995 Directive for the EU data protection system hardly needs explaining – and at any event was elaborated in detail in our previous paper while discussing the Commission's initial proposal on the draft Regulation.[37] In brief, Article 6 laid down the basic principles for the lawful processing of personal data, among which are such cornerstone notions for EU data protection such as the requirement for personal data to be processed "fairly and lawfully", the purpose limitation principle, the principle of proportionality or the data quality principle. All of them had to be observed by the data controller. On the other hand Article 7 set the criteria "for making data processing legitimate": it is through its provisions that individual consent was introduced in the data protection field, accompanied by other lawful grounds for personal data processing such as execution of a contract, legal obligation or the vital interests of the data subject concerned. A crucial clarification in this case pertains to the relationship between the two articles: namely, that their connection is conjunctive and not selective. Personal data needed to be processed according to the 1995 Directive's basic processing principles and also a lawful ground for the processing ought to be established. Data controllers could not opt to apply only one of the above articles in order for their operations to take place. Unfortunately this was not made crystal clear in the 1995 Directive's wording; a deficiency that we hoped would be corrected in the text of the Regulation.

In its initial proposal the Commission brought limited changes into the above basic scheme, mostly in the form of adding the principles of transparency and accountability to the list of data processing principles and relaxing the purpose limitation principle.[38] With regard to the connection between principles and lawful grounds for processing, it addressed the issue in an indirect way that definitely constituted an improvement in comparison to what was already in place but perhaps still allowed space for interpretations. Overall however its amendment of the principles and lawful processing grounds lists was self-limited and respectful of a system that was drawn in the pre-internet era and still operated adequately twenty years later.

From their part the Parliament and the Council more or less followed the Commission's approach on the above two matters. With regard to the processing principles, changes made by these two bodies were also limited: on what concerns terminology, each principle now carries its official name (in parenthesis, after being laid down in the Regulation's text), a blessing for legal scholars and practitioners who were always uncertain whether the same principles were referred to in the same way by everyone (for instance, the purpose limitation principle was also to be found as the purpose specification principle, etc.). Now the list is final, including altogether seven personal data processing principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and the accountability principle). From a substantive point of view changes mostly attributable to the Council refer to the strengthening of the special status awarded to research purposes personal data processing. In particular, "further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1), not be considered incompatible with the initial purposes" (Art. 5.1(b)). On the other hand, the principle of the necessity of the processing was moved from the body of the draft Regulation as suggested by the Commission to the Recitals (no. 30).

[36] See Article 24.
[37] See pp. 134–135.
[38] See Art 6.4 in its initial proposal.

Overall, if an assessment was to be made of their law-making intervention, the basic EU data protection principles, as included in Article 5 of the Regulation, gained a more meaningful title[39] and are worded in a more solid way, having reached their second generation and having found application to a multitude of different processing conditions over the past twenty years. Most importantly, the principles of transparency and accountability are welcome additions to their list that have been long discussed within the data protection community and are expected to offer substantially to individual protection. The warranting of the special status for research purposes is the result of experience gained over several years of data protection application to, and impediments on, scientific research. At the same time the reinstatement of essentially the same processing principles demonstrates consistence and offers legal certainty: the basic principles for the lawful processing of personal data as were known for the past twenty years remain more or less the same, having demonstrated the necessary resilience and flexibility in order to survive an increasingly complex data processing environment.

The same is more or less the situation with regard to Article 6 of the Regulation, where the lawful grounds for personal data processing operations to take place are laid down. Its par. 1 is maintained almost identical to that of the 1995 Directive and this has gone undisputed by all participating law-making bodies. Consequently, the lawful grounds for processing operations continue to be altogether six: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest, and overriding interest of the controller. Amendments of a rather secondary nature include the special treatment of children (with regard to overriding data controllers' interests) or the protection of the vital interests of any natural person (instead of the individual concerned, as was the case under the 1995 Directive).

Nevertheless, an important intervention seems to have occurred during the *trilogue* stage: a new Article (provisionally numbered 2a) has been inserted, warranting a significant level of autonomy to Member States. In particular, "Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with Article 6(1)(c) [compliance with a legal obligation] and (e) [public interest] by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX [processing relating to specific data processing situations]". While it is understandable that Member States may wish to maintain a level of autonomy while setting the conditions for the legal grounds of "legal obligations" or "public interest", according to which personal data processing may occur regardless of individual consent within their jurisdictions, the above new provisions seem superfluous: The paragraph that immediately follows, and has been present in the Regulation since the Commission's initial proposal, clarifies that for exactly the same cases (points (c) and (e) respectively), "the basis for the processing [. . .] must be laid down by (a) Union law or (b) Member State law". Subsequently, it offers further guidance, attributable to the Council, as to point (e) (public interest), as a lawful basis for personal data processing. Therefore, the insertion of a new paragraph 2a essentially repeating what was already stated in par. 3 of the same Article 6 appears at least confusing – and we consider that it should definitely not be interpreted as leading to a decrease of the level of protection but rather that the requirements of paragraph 3 are also applicable in what concerns paragraph 2a of the same Article.

The remaining of Article 6 of the Regulation is dedicated to the regulation of further processing (and as such could perhaps have been included in Article 5 above, but apparently the Commission's initial structure was followed by the Council and the Parliament). This exemption to the purpose limitation principle was present also in the first draft provided by the Commission and is after all considered a realistic approach in a processing era of, among others, ubiquitous computing, big data and the internet of things. The Regulation's wording follows what was suggested by the Council to this end; the Commission's initial wording was abandoned while the Parliament apparently did not agree with the idea of further processing at all and would have preferred for the relevant provisions to have been deleted. At any event, under paragraph 3a cases of personal data processing that is permitted despite not carrying the affected individuals' consent nor being allowed under a Union or Member State law are set: in this case the controller's relevant assessment needs to take into account, "inter alia", any links between the initial and the further processing purposes, the context of the collection of data, their nature, the possible consequences of the processing or the existence of appropriate safeguards. The list is indicative, so a controller might choose to take into consideration additional criteria. The fact remains, however, that further processing is indeed permitted under the Regulation, and it is up to the controller, according to the principle of accountability, to make the necessary evaluations as to whether the new, further processing, purposes are compatible with, and therefore permitted, the initials or not.

Finally, paragraph 5 of the initial Commission proposal was deleted. This is typical of a trend that can be met across the final text of the Regulation; in its initial proposal the Commission awarded itself perhaps a disproportionately important role with regard to implementation of the Regulation, through its self-authorisation to issue delegated acts on several application matters – as was for instance the case in this par. 5 where it awarded itself the power to regulate when the "overriding controller interest" legal ground for personal data processing would occur. Such self-promotion was (perhaps expectedly) not viewed favourably by the other two law-making bodies that strove to curb it as much as possible. In the case of this paragraph 5 they succeeded: after common petition by the Council and the Parliament the relevant provisions were deleted.

On the important issue of the connection between Articles 5 and 6 of the Regulation, as per the discussion on Articles 6 and 7 of the 1995 Directive outlined above, no change has been made with regard to the initial Commission proposal. Consequently, the relationship between the two is established as follows: Article 5 sets that "personal data must be processed

[39] "Principles relating to personal data processing" as opposed to the (partially misleading) "principles relating to data quality" of the 1995 Directive.

lawfully, [. . .]" and Article 6 sets that "processing of personal data shall be lawful only if and to the extent that at least one of the following [five legal bases] applies:" (6.1(a)). Therefore, all the principles of processing and a listed legal ground ought to concur on any personal data, in order for them to be lawfully processed. While this wording constitutes a definite improvement compared to that of the 1995 Directive, we believe that the Regulation would have benefited from an explicit link between the two Articles, perhaps in its recitals.

7. Individual consent: the Commission's request for "explicit" consent did not make it through (Article 7 of the Regulation)

Individual consent is arguably the most important legal ground for personal data processing to take place. All other possible legal grounds (performance of a contract, legal obligation, vital interests, public interest, overriding interest of the controller) refer to case-specific situations that lie more or less outside an individual's sphere of control; in a way, personal data processing under the remaining legal grounds listed in the Regulation takes place regardless whether the individuals concerned approve it or not. However, at the same time this is limiting also for data controllers: most of the processing operations that take place in routine transactional life cannot possibly be categorised under a legal obligation, or a vital interest, or a public interest, or even an important interest of the controller. Contracts evidently constitute an option but over the internet or on big data or internet of things implementations they are difficult to enter. Consequently, the vast majority of the mundane, daily, ordinary personal data processing operations surrounding us use individual consent as their legal ground, as per the request of Article 6 of the Regulation.

Because individual consent is therefore found at the basis of most personal data processing taking place around us, the ways its existence is established matter. As explained in our previous paper,[40] the past twenty years have witnessed fierce disputes between processing industries, who claimed that strict consent acquisition requirements are impossible to meet in the online, contemporary processing environment, and data protection proponents who insist on equipping each and every personal data processing operation with the individuals' concerned consent. Evidently, the requirement for individual consent was hindered with every year that passed: in an age of ubiquitous computing, big data, internet social networks and the internet of things, the idea that each data subject's consent needed to be procured for each processing operation happening appears more and more absurd. Nevertheless, on the other hand strict consent requirements are the last defence for individuals against the loss of control of the processing taking place with their personal information: the notification requirement becoming increasingly obsolete (and under the Regulation removed altogether) and the right to information being continuously streamlined to fit in new processing circumstances (see the analysis that follows), the only practical way an individual has in order to become aware that a controller is processing its data is when its consent is asked for it; the exercise of the rights to access and rectification (see analysis that follows) follows awareness that data are being actually processed in the first place.

In line with this prolonged debate, the Commission took a courageous standpoint in its initial proposal and asked for "explicit" consent. In our past paper we applauded its approach as a very important step towards an increase of the level of data protection afforded to individuals. Too bad then that after the Parliament's and Council's intervention this requirement has been removed from the final text of the Regulation.

Consequently, individual consent under the Regulation is "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed". Only the term "explicit" is missing from the initial Commission proposal – a small but crucial change. In comparison to the definition in the 1995 Directive changes are limited but, in their own terms, not insignificant. In particular, the addition of "unambiguous" and the requirement for a "statement" or "affirmative action" are important additions that build on past experience gained particularly with regard to various controllers' ingenious consent-collecting techniques used over the years (for example, pre-ticked opt-in boxes or implied consent in the event of entry into a contractual relationship, etc.). This is further explained in the Regulation's recitals: Recital 25 clarifies that individual consent should be given by means of clear, affirmative action "such as by a written, including electronic or oral statement". In even more detail, "this could include ticking a box when visiting an Internet website, choosing technical settings for information society services or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent". This constitutes valuable practical guidance and demonstrates that lessons from the past have been learned and incorporated into the text of the Regulation. While the term "explicit" has been removed, the listing above evidently constitutes the next-best option in order to warrant a significant level of protection and also not to appear irrelevant with the contemporary processing needs.

Other than that, Article 7 establishes that the burden of proof on existence of individual consent for a particular processing operation lies with the data controller; this is done in its paragraph 1, in a non-explicit way, in contrast with the initial Commission proposal. Paragraph 2 in the spirit of the newly introduced principle of transparency asks for "intelligible and easily accessible form using clear and plain language" in the event of "consent given in the context of a written declaration which also concerns other matters" – a praiseworthy attempt to protect individuals from contractual entanglements but otherwise a matter that could well fit into the Regulation's recitals. Paragraph 3 concerns consent withdrawal that can be given at any time but of course does not act retrospectively. Finally, paragraph 4, which could be read together with paragraph 2, evidently aims at reinforcing individual freedom to decide whether to consent to its data being processed in the event of "performance of a contract, including the provision of a service, is made conditional on the

[40] In p. 136.

consent to the processing of data that is not necessary for the performance of this contract".

The provisions on individual consent included in the text of the Regulation reflect the importance it gained over the past years. In practice the vast majority of personal data processing executed today is based on it, given that the remaining legal grounds for the processing are case-specific and therefore limiting. Expectedly therefore the Regulation expanded on it, dedicating a whole article to the particular conditions under which its existence can be established, either directly or indirectly by data controllers. It is exactly these indirect, implicit means for consent establishment that evidently pose the gravest difficulties. The initial Commission proposal was brave in defending individual rights and asked for "explicit" consent, but its standpoint was ultimately rejected by practically everybody else (the Parliament, the Council, the *trilogue* process). Perhaps this is justifiable, given contemporary processing circumstances; given this retreat, however, in order to accommodate them, we believe that application of these conditions that actually made it into the final text of the Regulation ought to be strict and guided towards warranting an increased level of data protection to individuals.

8. Updating the Directive's individual rights list (Art. 11–20 of the Regulation): the right to be forgotten (Art. 17 of the Regulation) following the CJEU Google Spain decision, profiling and other additions

One of the basic elements of EU data protection refers to a special set of rights granted to individuals in order to facilitate exercise of their right to data protection. In the text of the 1995 Directive these rights pertained to the rights to information, access and rectification of personal information (Articles 10, 11 and 12). Individuals were also afforded the right to object to personal data processing, evidently "on compelling legitimate grounds" as well as the right not to be subject to automated individual decisions (Articles 14 and 15 respectively). Technically this was performed in the following way: the individual right to information was divided into two cases, "information in cases of collection of data from the data subject", regulated in Article 10, and "information where the data have not been obtained from the data subject", regulated in Article 11. The right to access, regulated in Article 12, also included the right to rectification, regulated in 12(b). After an interval on "exemptions and restrictions", laid down in Article 13, the data subject's right to object was set in a separate Article (14) while the case against automated individual decisions was established in all of Article 15.

The Regulation essentially follows the same structure, adding however newcomers to the rights' list and providing far more detail on the "modalities" relevant to their exercise. In particular, Article 12 sets the way (the "modalities") that all of the following rights listed under Chapter III of the Regulation are to be exercised: the general principle of transparency is made concrete in the data subject's rights context, in its paragraph 1, and specific instructions are addressed to controllers, in the remaining paragraphs, on how to respond to data subjects' requests. While Article 12 may seem detailed, one must not forget that a Regulation needs to be a lot more precise because of its direct application effect. On the other hand it should be noted that the principles outlined in a general manner in the initial Commission proposal (in Article 11), which were later made concrete in the article that followed, were deleted while in the law-making process, leaving the remaining provisions somehow technical and cut-off.

Subsequently, the right to information is regulated again in two articles, as in the 1995 Directive, namely Articles 14 and 14a. Again distinction is made between cases where the information was obtained from the data subject and other cases. While the new wording broadly follows and expands what was known already under the 1995 Directive, attention should be given to the exemptions set in favour of data controllers when information is not obtained from the data subject: in this case, that is after all expected to be the norm under contemporary processing circumstances, the right to information does not apply, among others, when "the provision of such information proves impossible or would involve a disproportionate effort" and also as per Member State law. These are broad exemptions that could render in practice the right to information irrelevant. On the other hand, attention ought also be given to information to be provided in the event of further processing; in that case the controller needs to inform data subjects accordingly "prior to that further processing" (Art. 11.1b and 14a.3a).

The right of access occupies Article 15 in the Regulation. The wording more or less follows that of the 1995 Directive, including again reference to the right to rectification, in paragraph 1(e), that however by now is regulated in a single, standalone article, in article 16. Here again details are provided as to the actual exercise of the right to access information by individuals, in paragraphs 1b, and 2a. Consequently, Article 16 on the right to rectification merely serves as an explicit statement of what was otherwise derived from the text of the 1995 Directive: namely, that "the data subject shall have the right to obtain from the controller without undue delay the rectification of personal data concerning him or her which are inaccurate".

Moving to Article 17, on the "right to be forgotten", one could perhaps comment that these would have been the most anticipated, and widely discussed if not trademark, provisions of the Regulation, were it not for the recent CJEU Google Spain decision that dampened some of the Regulation's glory in that regard. At any event, Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers if specific conditions listed in its paragraph 1 are met (points a–f), among which is the withdrawal of consent. In the event that the controller has made such data public, reasonable steps will be taken to notify their recipients accordingly. Finally, the "right to be forgotten" (actually, to erasure of data) will not be applicable if it contrasts with the rights of freedom of expression and information as well as for several other, more expected, legal grounds (compliance with a legal obligation, public interest, archiving purposes, etc., as set in paragraph 3). While a detailed elaboration of this "right to be forgotten" largely exceeds the purposes of this analysis here it is enough to be noted that the final version of the Regulation is a far more moderate text than the one initially

suggested by the Commission.[41] A further point to be noted is that the Commission's (self-) authorisation to issue relevant delegated acts has been curbed (see the analysis above, under 6). At any event, the CJEU apparently took the data protection world by surprise when it established that a right to be forgotten was also at hand under the 1995 Directive's provisions in its landmark Google Spain decision. Accordingly, search engines in the EU have been removing search results upon individuals' relevant requests for the past two years and have accumulated useful practical experience to this end. The relationship therefore between the Regulation's right to be forgotten and the CJEU's reasoning in the above case will apparently require careful elaboration in the future.

Article 17a introduces a new notion in the exercise of data protection rights, that of the restriction of processing. In essence, it converted a paragraph of the initial Commission proposal (paragraph 4) into a standalone article and a relevant right. Data subjects have the right to have the processing of their personal data by controllers restricted, in the sense that such processing can only take place under strict conditions (defined in paragraph 2). The cases a restriction of the processing is applicable are listed under paragraph 1 and include a challenge of the accuracy of the data launched by the data subject, an objection as to the overriding interest of the controller for the processing (see above, under 7) or the intention of the controller to delete them while the data subject still requires them in relation to a legal claim. Despite its specific and technical character, the right to the restriction of processing might prove a useful tool while individuals form their legal remedy strategy, undertaking the role of injunctive measures in the data protection field.

The right to object is laid down in Article 19 of the Regulation (Article 18 and the right to data portability will be elaborated in the analysis that immediately follows). The exercise by an individual of its right to object to its personal data being processed by a controller essentially includes a balancing of rights and legitimate interests: on the one hand an individual is interested in having its data no longer processed (not necessarily deleted, however) and on the other hand a controller may have an interest in continuing to process such data despite the individuals' objections. This conflict was described in the text of the 1995 Directive (in its Article 14) and is still present in Article 19 of the Regulation: data subjects are afforded the right to object, but the controller "shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims" (paragraph 1). Other than that, Article 19 deals explicitly with personal data processing for the purposes of direct marketing, perhaps an inexplicable favourable treatment for this type of processing in today's ubiquitous computing environment that is however in line with the 1995 Directive provisions. An addition that apparently occurred during the trilogue refers to the obligation of controllers to inform data subjects on their right to object "at the latest at the time of the first communication" (paragraph 2b). Also, the Council's initiative to differentiate and treat with more flexibility personal data processing for historical, statistical or scientific purposes was ultimately adopted in the final text of the Regulation, in par. 2aa: by now, in the event of such processing individuals may indeed object but their application will not be successful if the processing is "necessary for the performance of a task carried out for reasons of public interest".

Finally, an important addition in the text of the Regulation refers to profiling.[42] Profiling is a widely debated topic: data protection proponents highlight its potential risks for individuals within the automated decision-making context; controllers on the other hand insist that its merits by far outweigh its disadvantages and that in any event it can be brought under strict regulatory controls in order to mitigate risks. The Regulation indeed adopted the latter point of view: it explicitly purports to regulate profiling, defining it under Article 4 and including it under the automated-decisions category. The initial Commission wording that was also in line with the 1995 Directive's approach on automated individual decisions in general (see its Article 15) is more or less adopted in the final text of the Regulation, admittedly under the more relaxed wording for data controllers as introduced by the Council. By now, the new rules do allow profiling operations to take place even based on sensitive data under the general, but not always applicable, condition that special measures for the protection of individuals have also been implemented.

9. The right to data portability (Article 18 of the Regulation) and the internet social networks market

The right to data portability is an internet-specific new right afforded to individuals in the text of the new Regulation. In practice it does not constitute a new right per se, because effective exercise of consent, and its withdrawal at any time, by data subjects would have presumably brought the same result. However, it may serve as a case-specific guidance both to individuals and controllers that is expected to affect in many and important ways the internet social networks market.

What the new right to data portability actually prescribes is that individuals are free to move around their personal data from controller to controller. Where this self-evident freedom under basic EU data protection law makes sense is the contemporary internet social networks environment. The relevant industry players spend much time and resources to encourage their registered users to create and deepen their profiles on their respective platform, but once this is done there is no easy way for the same users to extract their information and upload it to another controller – in essence, there is no easy way to change service provider. This is accomplished through technical measures or, better, through lack of them. System interoperability among internet social networks is missing, not only in Europe but globally. Internet social networks operate for the time-being as closed gardens for their users: once in

[41] For instance, the "abstention from further dissemination" or the "expiration of storage period" has been removed. Also, the whole of par. 2a is an addition attributable to the Council – as is however also the new Article 17b.

[42] See Hornung G, ibid, p. 73.

they enjoy all (free) functionalities, but they may never leave. The new Regulation chose to address this distortion in the market. Although it sounds more a competition than a data protection issue, the Regulation sets that "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided" (paragraph 1). Necessary conditions for this to take place is for the processing to be based on consent and for it to be carried out by automated means – definite pointers in themselves to the internet social networks environment. The final wording followed once again input from the Council closely, while an addition during the trilogue stage refers to the right of individuals to obtain that "the data is transmitted directly from controller to controller where technically feasible".

10. Data Protection Authorities (Art. 46 of the Regulation): in search of cross-border consistency

Data Protection Authorities (DPAs) constitute a pillar for the EU data protection model and are considered a successful mechanism for monitoring and enforcing data protection within their respective jurisdictions and it therefore comes as no surprise that their role is maintained and further strengthened in the text of the Regulation. However, the qualitative difference now refers to their (new) obligation to deepen their cooperation in order to achieve "consistent application of this Regulation throughout the Union" (Article 46, paragraph 2). This is inevitable given the fact that a Regulation has replaced the 1995 Directive, necessitating uniform application across the EU. The DPAs, being the basic implementation mechanisms, form an essential part of this effort. If they fail to apply the new provisions within their respective jurisdictions in a coherent and uniform manner then the much-anticipated harmonisation effect that led to introduction of a Regulation in the first place would be undermined. This is why every effort has been undertaken in the text of the Regulation to enhance cooperation and achieve a consistent approach on all data protection matters across the EU.

The other issue that DPAs, and the Regulation, had to face was the increasing cross-border nature of personal data processing. When the 1995 Directive was introduced the internet was practically unknown. Now personal data flow freely over it, seamlessly crossing jurisdictions, as transmitted by individuals themselves directly to controllers residing in any part of the globe. Inevitably data protection incidents became international. This refers both to jurisdictional and practical matters: residents of any Member State may find themselves in need to challenge the processing of controllers residing in another. Local DPAs, unless formally empowered with cross-border investigation powers, may offer very little to such disputes. The Regulation needed therefore to address these new processing circumstances – and also to coordinate its approach with the aforementioned need for consistent implementation across the EU.

Finally, it should also be taken into account that the Regulation's approach needs to be detailed on the establishment and operation of DPAs because it is intended to replace national data protection acts that otherwise would have catered for all such "functional" provisions.

It is under this light that the Regulation's provisions on DPAs ought to be read. Their aim generally follows their structure: their independent status and other institutional warranties are listed in Articles 46–49, their competences, tasks and powers are regulated in Articles 51–54, and the much-discussed co-operation and consistency mechanism is laid down in Articles 51a–62. A detailed analysis of these provisions exceeds by far the purposes of this paper. Here, apart from the above priority-setting that may be used as guidance while attempting to explain why a specific policy option was favoured over others, brief mention will only be made to the basic scheme adopted in order to face cross-border challenges and ensure consistent application of the Regulation provisions.

With regard to cross-border cases the basic notion of a "lead DPA" is introduced in the text of the Regulation: "the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing of this controller or processor" (Art. 51a). Consequently the basic criterion for designation of the lead DPA is the establishment of the controller or processor. While this sets the tone, and indeed an attempt to define what constitutes "main establishment" may be found in the Regulation's definitions (in Art. 4), brief mention ought to be made here to the fact that what constitutes "establishment" is a much debated issue even in front of the CJEU.[43] At any event, once a lead DPA is distinguished it shall "cooperate with the other concerned supervisory authorities in accordance with this article in an endeavor to reach consensus" (Article 54a). This is the basic notion of the so-called "one-stop-shop-mechanism" (see Recital 97c), evidently viewed from the point of view of international controllers who requested, and achieved, to have to deal with only one rather than all EU DPAs in the event their processing is cross-border. It is therefore on a mutual basis that may also include request for mutual assistance, that cross-border data protection incidents are intended to be treated under the Regulation. The process described in the Regulation is a possibly nuanced one, in order for decisions indeed to be reached by the lead DPA while also the opinions, and if needed intervention, of other interested DPAs will also be taken into account.

On the other hand, the Regulation's consistency mechanism is based on the European Data Protection Board (that will be discussed under 14, below). It is the Board's task to achieve consistency among EU DPAs, through its opinions prior to adoption of any substantial decision by a specific DPA (Art. 58). In other words, whenever Member State DPAs wish to adopt a substantial decision it must first alert the Board and acquire its prior opinion. While the Board's opinion is carefully named an "opinion" rather than a decision, the DPA concerned is obliged to "take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving

[43] See, for example, the CJEU Weltimmo and Google Spain decisions.

the opinion, electronically communicate to the chair of the European Data Protection Board whether it maintains or will amend its draft decision and, if any, the amended draft decision" (par. 8).

With regard to the law-making process, there is little point in attempting to follow changes brought in the Commission's initial proposal, because this issue (the consistency or one-stop-shop mechanism) has been one of the most disputed ones during its law-making passage. This is understandable not only from a realistic point of view (political and business expediency being at play here) but also from case law developments that occurred in the meantime: The Google Spain decision as well as the Max Schrems case (at the time of processing by the council anticipated, but its problematic on the one-stop-shop already visible, due to the fact that an Austrian citizen had to sue in Ireland) made a compromise among all interested parties and concerns necessary. Here it is only enough to be noted that the notion of a lead DPA was indeed present in the Commission's initial proposal. However, the multiple layers and procedures inserted in the Regulation compromise text in order to achieve a possibly balanced process that will not prejudice the powers and interests of other, non-lead DPAs are primarily inserted at the Council's initiative.

11. The obligation to notify replaced by the principle of accountability (Article 28 of the Regulation)

As discussed in our previous article, the obligation for controllers to notify all personal data processing operations taking place in the EU to their competent DPAs (see Art. 18 and 19 of the 1995 Directive) is an outdated and obsolete remnant of the 1960s and 1970s, when it was thought that processing operations would not be that many, would be country-specific and could therefore be organised in a centrally kept register. Reality has however proven otherwise; even since the 1990s the notification obligation was considered outdated.[44] Almost twenty years later the notification system could simply not be supported any longer. The initial Commission proposal, abolishing the duty to notify by means of not referring to it in its text, was not questioned either by the Parliament or the Council.

While there is no direct replacement for the notification obligation in the text of the Regulation, attention ought to be given to the shift towards the principle of accountability with regard to the controller (see Art. 5.2). By now, controllers are authorised to initiate personal data processing without notifying anyone, but it is their obligation to maintain an internal record (Art. 28) and to assess their processing so as to undertake, if applicable and equally at their own initiative, measures. While all this process remains internal to the controllers, who do not need to notify anything to anyone (unless of course a formal obligation for an impact assessment or prior consultation arises, see the analysis that follows), in the event of an investigation by a DPA they will be held liable if these measures have not been undertaken. In essence, this constitutes a reversal of the proof of burden in the text of the Regulation: while under the 1995 Directive controllers only needed to file a notification with the relevant DPA in order to be able to demonstrate lawfulness of their processing, under the Regulation they need to internally undertake appropriate safeguards which may of course never be challenged but which also, if ever questioned, they will need to be able to evidence.

12. Data breach notifications: made too flexible? (Articles 31 and 32 of the Regulation)

Data breach notification, as noted in our previous paper, is a data protection novelty that originated in the ePrivacy Directive[45] but in the meantime was considered a successful enough measure to find generalised use through introduction in the text of the Regulation (in Art. 31 and 32). A "personal data breach" is defined in the text of the Regulation as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Art. 4). When this happens, controllers need to assess the level of damage done: if they feel that the personal data breach is "unlikely to result in a risk for the rights and freedoms of individuals" then they may go ahead with their processing and not notify anyone on this event, taking however care to document it as best as possible in the event of future controls (Art. 31). However, if they think otherwise, then they need to notify their competent DPA not later than 72 hours after becoming aware of its occurrence. In the event that controllers feel that the same risk as above is "high" then they also need to notify the individuals concerned. However, even at this stage there are several options for controllers to avoid notifying individuals (and the subsequent "reputational sanction", see our previous paper), most notably one of which applicable ex post (making sure that the high risk "is no longer likely to materialise").

This layered approach, which allows substantial space for name-saving measures to be implemented by controllers at any stage of the data breach process, may ultimately render the reasoning behind data breach notifications, namely the shaming of the controller who failed to undertake sufficient security measures, obsolete. If controllers are afforded with a three-level approach the culmination of which, rather than the norm, being the notification of the individuals concerned, and even that is watered down by additional parameters ("disproportionate effort") and *ex post* measures, then in practice very few notifications are expected to indeed reach the public in a meaningful format. The compromise text constitutes a significant reduction of the safeguards foreseen by the Commission in its

[44] See Simitis S, Die Erosion des Datenschutzes – Von der Abstumpfung der alten Regelungen und den Schwierigkeiten, neue Instrumente zu entwickeln, in Sokol B (ed.), Neue Instrumente im Datenschutz, Dusseldorf 1999, p. 20.

[45] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, pp. 37–47.

initial proposal (for example, the initial proposal made in principle all data breaches notifiable to the DPAs and moved the risk threshold a notch lower, not distinguishing between a risk and a high risk). It remains to be seen whether this significant flexibility afforded to controllers will contribute or not to the data protection purposes – given also that data breaches are of journalistic interest and indeed it was through these means that the public was informed until today of relevant compromises of its data protection rights.

13. The role of "soft law": Data Protection Impact Assessments, codes of conduct and certification (Art. 33, 38 and 39 of the Regulation)

Among the many novelties introduced by the Regulation, "soft law" instances in the form of Data Protection Impact Assessments, codes of conduct and certification hold a prominent position. These newcomers ought to be examined within the context of the abolition of the notification system and the introduction of the principle of accountability instead; under the Regulation, controllers are expected to take the initiative with regard to their personal data processing. Such initiative however could include a substantial cost that could burden disproportionately small companies. The above three tools could provide valuable flexibility in this context. Despite their common functionality, each one of the above regulatory tools has a different background: Data Protection Impact Assessments is an idea originating from the positive experience of environmental, regulatory and social impact assessments that were suggested as a useful addition in the data protection field, at least in Germany, since the mid-1990s.[46] Codes of conduct were mentioned in the text of the 1995 Directive, without however gaining much attention in practice over the past twenty years. Finally, certification in the data protection field is an idea first developed in the USA that recently found various implementations in the EU, without however a firm theoretical, practical or legal ground.

As far as Data Protection Impact Assessments are concerned, they are introduced as a mandatory exercise in the event that a controller, to its own judgement and assessment, finds it "likely to result in a high risk for the rights and freedoms of individuals" (Art. 33 par. 1). The cases that this could occur are indicatively listed in the Regulation: these pertain to the "use of new technologies" also "taking into account the nature, scope, context and purposes of the processing"; in this context cases that definitely fall under this category refer to profiling or to any "systematic and extensive evaluation of personal aspects", the processing of sensitive data or the large-scale monitoring of a public area (par. 2). At any event, the impact assessment ought to be drafted prior to undertaking such processing. Further guidance as to the contexts and the process of drafting such a report is provided for in the text of the Regulation; its analysis largely exceeds the purposes of this text. Here it is enough to be noted that changes brought to the initial Commission proposal are more of an explanatory nature, perhaps the most important among them pertaining to the clarification that "a single assessment may address a set of similar processing operations that present similar high risks" (par. 1, apparently at the suggestion of the Parliament). Data Protection Impact Assessments are expected to be expensive to carry out and will expectedly burden indiscriminately any controller undertaking risky processing. This will include also SMEs or even startups engaged in the relevant fields. Data Protection Impact Assessments of a "horizontal" scope, to cover for an entire "similar processing operations" field (assuming in a way the role of a code of conduct for a more focused field of application), could constitute a welcome attempt to alleviate their financial burden and provide flexibility.

Codes of conduct should be placed within the same framework: that of providing assistance to small companies while applying the Regulation. During its law-making passage a lot of criticism was guided towards the perceived increased financial burden for SMEs that will need to apply its provisions. A direct reply to such criticism may be found within the Regulation's provisions in codes of conduct: these are specifically intended to "take account of the specific needs of micro, small and medium-sized enterprises" (Article 38, par. 1). Codes of conduct constitute mostly self-regulatory instruments, whose self-regulatory level is dependent upon the degree of ratification they are expected to receive by DPAs or other state authorities. They were included in the text of the 1995 Directive, occupying a whole article (Article 27), with the purpose to "contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors". However, despite their worthy intentions to regulate in a concrete and case-specific manner the personal data processing undertaken by separate industries, they were left in obscurity ever since: to-date no significant relevant codes exist, except perhaps from a few industry sectors.[47] However, their potential contribution to the data protection purposes was deemed so important as to include them, this time in more detailed format, also in the text of the Regulation. The initial Commission proposal was furthered mostly in a technical manner by the other two law-making bodies, with the important addition (following the Council's input) on "monitoring approved codes of conduct" (Art. 38a). Essentially, the monitoring of compliance with a code of conduct may be "carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority". This is a useful addition towards the direction of institutionalising otherwise self-regulatory sets of rules freely devised by the industries concerned.

Finally, certification is a newcomer in the data protection field: despite of the fact that it was being discussed over the past ten years as a useful addition, the fact is that the idea originates from the USA where self-regulatory certification mechanisms are in place since the 1990s. This is however the only common point to be found between the US and the EU

[46] See Rossnagel A, Datenschutz-Audit, in Sokol B (ed.), Neue Instrumente im Datenschutz, Dusseldorf 1999.

[47] Direct marketing being one of them, see FEDMA's European Code of Practice for the Use of Personal Data in Direct Marketing, available at http://www.fedma.org.

approach on this matter: the certification model prescribed in the Regulation is a formal one, placed under the direct or indirect scrutiny of the competent DPAs that has little to do with the entirely self-regulatory system applied in the USA. According to par. 1 of Article 39, "The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account". Certification therefore is also intended to assist small enterprises in complying with the Regulation. A preference for an EU system, a European Data Protection Seal" is also made clear in the Regulation's text. While the details of the implementation also exceed the purposes of this analysis here it is enough to be noted that, after the law-making process, the initially open approach introduced by the Commission, which could accommodate various alternatives that would presumably be finalised in relevant delegated acts issued by the Commission, has now been replaced by a concrete model (as per the combined reading of Articles 39 and 39a) whereby a certification shall be issued by certification bodies on the basis of criteria adopted by the competent DPA or by the DPA itself.

14. The European Data Protection Board as a consistency gatekeeper (Article 64 of the Regulation)

The importance of the Article 29 Working Party for the EU data protection cannot be overstated.[48] During the past twenty years since its introduction in the text of the 1995 Directive it has constituted the main body for consultation and harmonisation on all data protection matters within the EU. Although of a consultative nature, the fact that its members were Member State DPAs meant in practice that the level of influence over data protection implementation across the EU follows only Court decisions or new regulatory instruments. After all, a recent show-case of its strength is the deadline set by it for the replacement of the Safe Harbour Agreement, annulled by the Court that was promptly observed by the negotiating parties.

However under a Regulation environment the role of the Article 29 Working Party unavoidably required an overhaul. The direct effect of the Regulation, which will however be implemented at Member State level by twenty-nine different DPAs, unavoidably raises questions of harmonisation. A consistency mechanism is the only conceivable way through which such harmonised application across the EU could be achieved. This role has been granted to the European Data Protection Board: "In order to promote the consistent application of this Regulation, the European Data Protection Board should be set up as an independent body of the Union. To fulfill its objectives, the European Data Protection Board should have legal personality" (Recital 110). The scheme upon which the consistency mechanism will be based is straightforward: whenever a DPA wishes to reach an important decision, it must first secure the prior (positive) opinion of the Board (Article 58). The Board is also made responsible to address any disputes raised among DPAs by means of a binding decision (58a). In this way the Board, where again all Member State DPAs are represented (Article 64), is strengthened if compared with the Article 29 Working Party it replaces so as to become the highest executive data protection monitoring party in the EU.

Apart from its role in the Regulation's consistency mechanism the Board maintains the consultative function that its predecessor holds under the 1995 Directive. The catalogue included in Article 66 is long, and at the same time indicative ("in particular"): new powers could be added to an already long list extending from advising the Commission and issuing best practices in order to encourage consistent application of the Regulation to issuing guidelines on profiling, binding corporate rules, data breach notifications or even codes of conduct and certification schemes. Another important point is that the Board may assume all these powers either at the request of the Commission or "on its own initiative".

The outcome of the law-making process was undoubtedly favourable to the Board. Where the initial proposal of the Commission perceived a Board with more or less the same powers as the Article 29 Working Party and mostly dependent upon the Commission itself, essentially requiring it to forward all its opinions and recommendations to the Commission for further actions, the end result of the law-making process is a strong and standalone Board with legal personality that is capable of deciding on itself and enforcing its opinions. In a way it could be held that the shift of power away from the Commission, through deletion of most of its powers to issue "delegated acts" in the text of the initial proposal, moved towards the Board that assumed in essence the role that the Commission would presumably have liked to have kept for itself. At any event, the fact remains that the new Regulation introduces an important new player in the EU data protection scene, upon which essentially all hope for the success of the Regulation's direct effect is vested.

15. Conclusion: still a sound system for the protection of individuals

Four years ago we concluded that the release of the new Regulation draft was a "cause for celebration for human rights". Obviously, the question is now whether the Regulation's final wording still justifies our previous finding. In short, we believe that it does. Even the choice of legal instrument, a Regulation instead of a Directive, is reason enough to celebrate: inconsistencies and lack of harmonisation that attracted so much attention over the past decades and led to impasses due to technological developments and internet business trends now finally have the means to be addressed in an effective and satisfactory way. In addition, a bunch of data protection novelties demonstrate that due care has been taken for future requirements as well: the right to be forgotten, the right to data portability, data protection impact assessments, codes of

[48] See also Blume P/Svanberg C W, ibid.

conduct, certification, privacy by design and others, all add to the EU data protection dictionary, if not arsenal, and are guided towards anticipated personal data-intensive processing. In the same context, law-makers did not hesitate to incorporate into the Regulation lessons of the past, for example by deleting the obligation to notify and by strengthening the principle of controllers' accountability.

However the above constitute merely an opportunity and not a necessary and inevitable development. The Regulation will come into effect within two years and a lot of work needs to be done by all EU institutions in the meantime through releasing the necessary implementing acts. Too many things can go wrong: the consistency mechanism may not work, causing fragmented implementation of the same provisions in different Member States. Or, the one-stop-shop could not function properly, creating tension among DPAs and despair to cross-border controllers. Or, these implementing acts may simply take too long to be released, delaying their intended processing-friendly effect and leaving controllers only with new obligations and no way to apply them in a simple way in practice. The Regulation is offering the tools with which to address problems of the past and boldly face the future; the use we make of them is entirely up to us.

With regard to the law-making process itself, a lot of things changed since the Commission released its initial proposal back in 2012. Among the most notable changes could be listed the shift of power from the Commission towards the European Data Protection Board or the overhaul of Chapter IX, on the "specific data processing situations" (a chapter that was regretfully not analysed above, due to space constraints). While one could not possibly generalise upon the character of the Council's or the Parliament's interventions, easily noticeable traits refer to the fact that the Regulation's final wording follows more the Council's approach than that of the Parliament (a fact partly attributable to the fact that the Council formulated its opinion last, taking note of the Parliament's already published position) and that the Council's approach was more technical and realistic whereas the Parliament attempted to address more fundamental issues with regard to the initial proposal. The trilogue process made few but substantial changes into the final document.

An important point that is the result of the law-making process refers to the fact that a new data protection industry emerges. The technical nature of interventions brought to the initial proposal, which the Commission perhaps intentionally left more abstract to be completed by delegated acts, if read conjunctively reveals substantial legal incentive to create a new industry with regard to application of the Regulation: data protection officers, accreditation bodies for codes of conduct and certification, impact assessments, are all important tasks that will require experts and new organisations in order to execute properly. While the potential financial burden upon controllers created by the Regulation needs also to be taken into account, if seen from a different perspective the Regulation instructs that a whole new industry be created, complete with its own professionals, products and marketable (and even exportable, under certain circumstances) services.

While this is probably not the place to mourn for the loss of the 1995 Directive, a brief mention to its invaluable contribution to EU and global data protection ought nevertheless to be made. The Directive constituted the international standard against which all data protection initiatives in and out of Europe were judged. While it was frequently felt that it set the data protection bar too high, its basic components (processing principles, conditions for the lawfulness of the processing, data subjects' rights, establishment of data protection authorities and the rules on cross-border data transfers) are in one way or the other addressed in all data protection instruments around the globe. In this way, it set the data protection structure globally. Finally, it did not cease to show its teeth and surprise us even twenty years after its release, as recent Court of Justice decisions based on its provisions demonstrate. On the other hand, its replacement was long overdue: being drafted in the pre-internet era several of its provisions had in the meantime become irrelevant and even the Court's recent teleological approach was not sufficient enough to hide their age.

As frequently noted, this paper constitutes the continuation of our previous one of 2012 commenting on the Regulation's initial draft. From this point of view account needed to be taken of our previous structure in order to be able to demonstrate parallel developments and draw meaningful conclusions. However, the Regulation is an ambitious and long text intended to cover all personal data processing aspects within the EU. There are therefore many angles from which to view and present its provisions. Important issues that we would have liked to comment but were deemed inadvisable due both to space constraints and structure limitations refer to, indicatively, international data transfers, the processing for academic, scientific, historical and related purposes, the prior co consultation requirement, or the role of data protection officers. While this is a task left for the future, mere mention of such important elements of the Regulation that did not fit in this analysis serves as further evidence of the fact that it constitutes an ambitious text whose release justifiably took more than five years to complete that is planned for a life span and far-reaching effect to match at least the impressive record of its predecessor.